gsmの解読可能性 (情報科学の数学的理論)

AUTHOR(S):

佐藤, 興二

CITATION:

佐藤, 興二. gsmの解読可能性 (情報科学の数学的理論). 数理解析研究所講究録 1972, 156: 111-132

ISSUE DATE:

1972-08

URL:

http://hdl.handle.net/2433/106856

数理解析研究所講究録
156巻 1972年 111-132

gsmの解読可能性

京大 理　佐藤興二

§1. 序

一般に，transducer Mによる記号系列の写像をfとするとき，ある形式言語Lに対して，f(L)上での写像f^{-1}の価数が有界であるとき，MはLに対して有限義解読可能であるという。又，その価数を有限義解読可能性の次数といい，次数がnなら，n義解読可能という。Mが，補助記憶をもたない一方向オートマトン，すなわち一般化された順序機械(gsm)であるとき，Lが文脈自由言語ならば，下に示す通り，MがLに対して有限義解読可能であるか，一義解読可能であるか等の判定は一般に可解でない。

ここでは，Mがgsm，Lが正規集合であるとき，これらの決定問題が，非決定性有限オートマトンによって定義された正規集合の，系列の受理の仕方(初期状態から最終状態へ達する道筋)の多様度を評価する問題に帰着されることを示し，実際のアルゴリズムをのべることによって，これらが決定可能であることを示す。又，関連あるいくつかの結果についてものべる。

§2. 諸定義及び問題の帰着.

1. 与えられたgsm $\mathfrak{M}=\langle K_M, \Sigma, \Delta, \delta_M, \lambda_M, Q_0\rangle$(註1) と形式言語 $L\ (\subset\Sigma^*)$ に於て, $\mathfrak{M}$の任意の出力系列 $y\in\Delta^*$ に対して, yを出力とするような入力系列のうちLに属するものの数が常に有限の確定した値nを越さず, かつnより小さな数では押さえられないならば, $\mathfrak{M}$は言語Lに対してn義解読可能である又は言語Lは$\mathfrak{M}$-n義であるという。又一般にそのようなnが存在するとき, $\mathfrak{M}$はLに対して有限義解読可能(finitely decipherable)である又はLは$\mathfrak{M}$-有界であるといい, nを(有限義)解読可能性の次数という。

2. $\mathfrak{M}$の任意の出力系列 $y\in\mathfrak{M}(L)$ と, yを出し終ったあとの$\mathfrak{M}$の最終の状態から, 対応する入力系列で言語Lに属するものが常に一意的に決まるならば, $\mathfrak{M}$はLに対して情報無損失である又はLは$\mathfrak{M}$-無損失であるという。$R(Q_j)$ $(Q_j\in K_M)$ を, $\mathfrak{M}$をQ_0からQ_jへ到達させる入力系列の全集合とするとき, Lが$\mathfrak{M}$-無損失であるとは, 全ての$Q_j\in K_M$について, $L\cap R(Q_j)$が$\mathfrak{M}$-1義なることと同義である。したがって$\mathfrak{M}$-無損失は$\mathfrak{M}$-有界の特殊な場合であり, その次数は$\mathfrak{M}$の状態数を越えない。

3. Lが$\mathfrak{M}$-1義であるということは, $\mathfrak{M}$の出力側にあって, 出力系列から対応する入力系列を解読しようとする"decoder"が, もし入力系列が常にLに属しているということを知っていたら, 一意的にdecodeできるということである。このことは更に次のように一般化できる。すなわち, 包含関係のある2つの形式言語L, M $(L\subset M)$と, gsm $\mathfrak{M}$に於て, $y\in\mathfrak{M}(L)$なる任意の出力系列に対して, 対応する入力系列がMに属するということを知っているだけで,

decoderが一意的に解読できるとき，Lは M をヒントとして MI-1義であるという。したがって，L が MI-1義であるとは，L が L 自身をヒントとして MI-1義であるということと同義である。MI-n義，MI-有界，MI-無損失等についても同様のことが定義できる。

以上の定義は形式的には次のようになる。

$L \subset \Sigma^*$ に対して，$D_n^{MI}(L)$ $(n=1,2,3,\cdots)$ は次のような系列の集合を指すとする。

$$D_n^{MI}(L)=\{x\in L \mid \exists x_1, x_2, \cdots, x_{n-1}\in L,\ MI(x)=MI(x_i)\ \ {}^\forall i=1,\cdots,n-1\}$$

但し，$x_i \neq x$，$x_i \neq x_j$ if $i \neq j$

L が MI-n義であるとは $D_{n+1}^{MI}(L)=\phi$，かつ $D_n^{MI}(L)\neq\phi$ なることである。

又，$L\subset M$ なるとき，正整数 n が存在して

$$D_{n+1}^{MI}(M)\cap L=\phi$$

かつ $D_n^{MI}(M)\cap L\neq\phi$　したがって　$L\subset M-D_{n+1}^{MI}(M)$

ならば，L は M をヒントとして MI-n義である。

4.　L が MI-1義であるとき，$L'\supsetneqq L$ なるいかなる L' も MI-1義でないならば，L は極大MI-1義集合であるという。MI-n義，MI-無損失についても同様。L が極大 MI-1義集合であるための必要充分条件は，L が MI-1義であって，かつ $MI(L)=MI(\Sigma^*)$ なることである。

系1．L が極大MI-無損失集合であるための必要充分条件は，全ての $Q_j\in K_M$ について，$L\cap R(Q_j)$ が MI-1義であり，かつ $MI(L\cap R(Q_j))=M(R(Q_j))$ なることである。

系2．$A\equiv\Sigma^*-D_{n+1}^{MI}(\Sigma^*)$，　$B\equiv L\cap D_{n+1}^{MI}(\Sigma^*)$ とする。
L が極大 MI-n義集合であるための必要充分条件は ① $L\supset A$　② $MI(B)=MI(D_{n+1}^{MI}(\Sigma^*))$ ③ $D_n^{MI}(B)=B$　④ $D_{n+1}^{MI}(B)=\phi$　を全て満たすことである。

定理.1.　任意の順序機械$\mathfrak{M}$と文脈自由言語Lの組$(\mathfrak{M}, L)$について，$\mathfrak{M}$がLに対して

① 有限義解読可能であるか

② 一義解読可能であるか

③ 情報無損失であるか

④ Lが極大$\mathfrak{M}$-1義集合であるか，極大$\mathfrak{M}$-無損失集合であるか

を判定するアルゴリズムは存在しない。

証明．τ_α, τ_βを，$\tau_\alpha(x) = \langle x, \alpha \rangle$，$\tau_\beta^{(x)} = \langle x, \beta \rangle$，$\forall x \in \Sigma$，~~$\alpha, \beta \notin \Sigma$~~
なるようなhomomorphism $(\Sigma^* \to (\Sigma \times \{\alpha, \beta\})^*)$，
$\mathfrak{M}$を，$\mathfrak{M}(\langle x, \alpha \rangle) = x$，$\mathfrak{M}(\langle x, \beta \rangle) = x$　$\forall x \in \Sigma$ ~~なるような~~
なるようなhomomorphism $((\Sigma \times \{\alpha, \beta\})^* \to \Sigma^*)$とする。
L_1, L_2を任意の2つの文脈自由言語とするとき，$L = \tau_\alpha(L_1) \cup \tau_\beta(L_2)$は文脈自由言語であり，$\mathfrak{M}$は，明らかに，$L_1 \cap L_2 = \phi$なる時及びその時にのみ$L$を単射する。任意の2つの文脈自由言語$L_1, L_2$に対して，$L_1 \cap L_2 = \phi$か否かは決定不能であるから，$\mathfrak{M}$が$L$を単射するか否かは決定不能である。$\mathfrak{M}$は状態が1つの順序機械と考えられ，したがって一義解読可能性と無損失性は一致するから，よって②③が決定不能であることが証明された。

①が決定不能であることは，文脈自由言語がconcatenation及び$*$について閉じていることより証明できる。$\mathfrak{M}$を与えられたhomomorphism $\Sigma^* \to \Delta^*$とするとき，
$\mathfrak{M}'$を次のようなhomomorphism $(\Sigma \cup \{\alpha\})^* \to (\Delta \cup \{\alpha\})^*$，$(\alpha \notin \Sigma \cup \Delta)$とする。

$$\mathfrak{M}'(x) = \mathfrak{M}(x) \quad \forall x \in \Sigma$$
$$\mathfrak{M}'(\alpha) = \alpha$$

このとき，Lを任意の文脈自由言語とすると，文脈自由言語$(L\alpha)^*$ $(L \subset \Sigma^*)$が$\mathfrak{M}'$-有界であるための必要充分条件はLが$\mathfrak{M}$-1義なることである。よって②に帰着された。

次に$\mathfrak{M}$をidentity machine（すなわち$\mathfrak{M}(x) = x$　$\forall x \in \Sigma$）とすると，文脈自由言語Lが極大$\mathfrak{M}$-1義集合（極大$\mathfrak{M}$-無損失集合）なることは，$L = \Sigma^*$なることと同値である。よって④は決定不能。　Q.E.D.

以下，Lが正規集合である場合を扱う。

与えられた正規集合 L を受理する（決定性）有限オートマトンを $A=\langle K_A, \Sigma, \delta_A, q_0, F\rangle$（註2）とする。

gsm M と有限オートマトン A から定義される次のような積機械 M×A を考える。

$$M\times A = \langle K_{M\times A}, \Sigma, \delta_{M\times A}, \lambda_{M\times A}, \widehat{Q_0}\rangle$$

1) $K_{M\times A} = K_M \times K_A$

2) $\delta_{M\times A}((Q_i, q_j), x) = (\delta_M(Q_i, x), \delta_A(q_j, x))$

$\lambda_{M\times A}((Q_i, q_j), x) = \lambda_M(Q_i, x)$

$$(\ Q_i \in K_M,\ \ q_j \in K_A,\ \ x \in \Sigma\ )$$

3) 初期状態 $\widehat{Q_0} = (Q_0, q_0)$

積機械 M×A は，2つの機械 M と A を単に並列させたもの（図1）で，その入出力関係については M と等価（homomorphic）な機械であり，M の内部状態に A の状態の各々を組み合わせることによって，状態の redundancy を増したにすぎない。又同様に，M×A の状態の "A-成分" にのみ注目すれば，これは A と等価なオートマトンであることも明らかである。そこで，A-成分がオートマトン A の最終状態であるような M×A の状態を，M×A の "最終状態" と呼ぶことにし，M×A の状態遷移図から入力文字を消し，出力文字にのみ注目すれば，これは出力アルファベット上の正規集合 $M(L)\subset\Delta^*$ を定義する非決定性有限オートマトンであると見なせる。今，$y\in M(L)$ とするとき，この非決定性有限オートマトン M×A によって y が受理される仕方，すなわち初期状態から状態遷移図の矢印をたどって最終状態へ到達する道筋は，一般に2つ以上存在するが，M は決定性 gsm であるから，それらの道筋の各々に対して異なった入力系

列が対応していることは明らかである。したがって，正規集合Lが MI-有界であるか否かの判定は，$y \in MI(L)$ に対するこれらの受理の道筋の多様度が $MI(L)$ 上で有界であるか否かの判定に帰着されることになる。

MI-n義，MI-無損失の判定についても同様であって，前者は，道筋の多様度が常にnを越さないか否かの判定，後者は，$y \in MI(L)$ と，yを受理する MI×A の最終状態の MI-成分から一意的に道筋が決まるか否かの判定と等価である。

そこで，MI×A の遷移図に於て，1つの状態遷移（矢印）に長さ2以上の出力系列がともなう場合は，途中，出力の一文字ごとに temporary な状態をつけ加え，それらの temporary な状態間の遷移にともなう入力は ϵ（無入力）とする。（図2） 更に，このようにしてできた遷移図の遷移（矢印）に各々異ったlabelをつける。このようなlabelの集合を $T = \{t_1, t_2, \cdots, t_r\}$ とする。（rは矢印の数に等しい） このようにすると，遷移図は，Tを入力アルファベットとする決定性有限オートマトンと考えられ，MI×A を初期状態から最終状態に到達させる遷移の系列は，ある正規集合 $P \subset T^*$ をなす。各遷移 $t_i \in T$ に，それにともなう入力文字（ϵを含む）を対応させる写像をσ，出力文字（ϵを含む）を対応させる写像をτとするとき，σ，τを，homomorphism として T^*上に拡張するならば，PとLは homomorphism σ によって1対1の対応をなし，（したがって $\sigma(P) = L$），又，$\tau(P) = MI(L)$ となる。

よって，正規集合Lが MI-有界か否かの判定は，正規集合Pが τ-有界か否かの判定に帰着されるが，ここで注意すべきことは，τが $|\tau(t_j)| \leq 1$ $\forall t_j \in T$ なる homomorphism であることである。このような homomorphism

を"短縮homomorphism"と呼ぶことにする。

以下，短縮homomorphismの，一般の正規集合 $P \subset T^*$ に対する有限義解読可能性の判定法をのべる。

§3. 短縮homomorphismの正規集合に対する解読可能性

与えられた短縮homomorphismを τ，正規集合 $P \subset \Sigma^*$ を受理する有限オートマトンを $B = \langle K_B, \Sigma, \delta_B, q_0, F_B \rangle$ とする。

P が τ-有界か否かを判定するアルゴリズムを，例をあげて述べる。

まず，τ が ϵ-free の場合（すなわち $|\tau(x)|=1 \ \forall x \in \Sigma$，この場合 τ は系列長を保存する）について説明し，$\exists x \in \Sigma, \tau(x)=\epsilon$ なる場合は，後で補足的に説明する。

Notation；ある $q_j \in K_B$ について，$q_j \notin F_B$ であり，かつ $\forall x \in \Sigma^*, \delta_B(q_j, x) \notin F_B$ なる場合，q_j を ϕ-状態という。B が reduced machine であるなら，ϕ-状態は高々1つである。

1. まず P を受理するオートマトン B の reduced diagram に，ϕ 状態が存在するなら，それを消し，ϕ-状態への矢印（遷移），ϕ-状態からの矢印も共に消す。次に各矢印に付随している入力文字を消し，かわりにその入力文字のhomomorphism τ による出力 $\in \Delta$ を書き込む。この出力図を G とする。図3.は ϕ-状態以外の状態が強連結であるような出力図の例である。最終状態は $\{q_1, q_2, q_3\}$ とする。

2. 出力図 G から，初期状態 q_0 から始まって，同じ出力をともなう可能な状態遷移の様子を示す tree状の図をつくる。これを"test tree"と呼ぶことにする。これは非決定性オートマトンから決定性オートマトンをつくる時の手順

と同様のものである。図4.は図3.の test tree である。いくつかの状態が $\boxed{}$ (boxと呼ぶ)でかこんであるのは出力が同じであることを意味しており、各boxの左下の文字はその共通の出力を示す。各boxからは、最大限出力文字数と同数のboxが派生することになる。test treeをつくる手続きは無限に続ける必要はない。何故なら、あるboxと同じ種類の(すなわち全く同じ状態を含む)boxが、そのboxの"先祖"に存在したら、あとは同じことの繰り返しで、一種のloopに陥るからである。例えば第3列、第4列の $\boxed{0\ 1}$ は第2列に、最終列の $\boxed{0\ 1\ 3}$, $\boxed{0\ 2\ 4}$ はそれぞれ第6列、第5列に同じものが存在する。

さて、この例の場合、test treeにあらわれるどの状態に対しても、図5のように2つ以上の矢印が同時に向かっているようなことはない。そのような、2つ以上の矢印が合流する状態がtest treeに存在する場合は、その点を"結節点"と呼ぶことにする。結節点が存在するということは、test treeに於て、初期状態 q_0 から、その結節点の状態(q_j とする)へ到達する道筋が2つ以上あるということである。これらの道筋が共通の出力をともなっていることはtest treeの構成から明らかであり、道筋が異なれば対応する入力が異なるのは当然であるから、これはPが τ-1義でないことを意味する。何故なら $y\in\Delta^*$ を共通の出力、q_j から任意の最終状態へ到達する系列(q_j は ϕ-状態でないから、そのような系列は存在する)を $x\in\Sigma^*$ とするとき、$y\tau(x)$ は少くとも2義に解読されるからである。

この例では、test treeに結節点が存在せず、かつ各boxに含まれる最終状態の数は最大2($\boxed{0\ 1\ 3}$ の1と3)であるから、どのような長い出力系列も $\tau(P)$

に対しても，それを出力とする入力系列で，$\mathbb{B}$を最終状態へ導くようなものは，高々2通りしかないことがわかる。よって $\mathbb{P}$は τ-2義である。

もし，全ての状態が最終状態なら $\mathbb{P}$は τ-3義となる。

命題1．出力図Gの test tree に結節点が存在しなければ，$\mathbb{P}$は τ-有界であり，その次数は，各boxに含まれる最終状態の数の最大のものに等しい。

特に，Gが強連結ならば

1) test tree に結節点が存在しないことが，$\mathbb{P}$が τ-有界であるための必要充分条件である。

2) $\mathbb{B}$の最終状態の数を n とするとき，$\mathbb{P}$が τ-有界ならば その次数は高々 n である。

3) $\mathbb{P}$が τ-有界ならば，$\mathbb{B}$の初期状態を変えて得られる新しい正規集合も τ-有界であり，その次数は変わらない。

1)の証。　充分なることは明らか。逆に，test tree に結節点が存在するとする。結節点の状態を $q_j \in K_B$ とするとき，

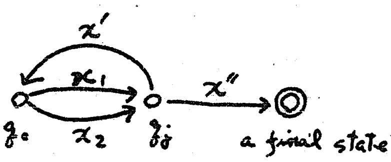
$\exists x_1, x_2 \in T^*,\ x_1 \neq x_2$
$\qquad \tau(x_1) = \tau(x_2)$ ($= y$ とする)

q_jから初期状態 q_0への任意の入力系列を x'

q_jから任意の最終状態への入力系列を x''

(Gが強連結なることより，x', x''は必ず存在する)

とすると，



$$(y\tau(x'))^n \tau(x'') \in \Delta^*$$

を出力とするような入力系列で，$\mathbb{P}$に属するものは少くとも 2^n 通り，すなわち，

$\{(\prod_{j=1}^{n} (x_{i_j} x'))x'' \mid i_j = 1 \text{ or } 2\}$　存在する。　$n \to \infty$ で $2^n \to \infty$。

2) 3) は 1) より明らか。

したがって，前節で述べたことより，

命題2．積機械 M×A が強連結ならば、Aの最終状態の数を m，Mの状態数をnとするとき，MのLに対する有限義解読可能性の次数は mn を越えない。

3．次に，一般に，出力図Gが強連結ではなく，かつ test tree に結節点が存在する場合であるが，Pがτ-有界でないということは，"結節点の無限の連なり"が存在して，出力系列が長くなるにつれて，結節点を含む box を通る回数が多くなり，そのたびに対応する入力系列の道筋が増加していくということである。(註3) したがって，結節点が存在する場合は，それらの結節点が test tree に於て，どのように互いに連結されているか（すなわち矢印で結ばれているか，間接的でもよい）を調べる必要がある。図6．の G_2 は強連結でない出力図の例であるが，その test tree（図7）で ②③④ の④及び ①③④ の③は結節点である。前者をA，後者をBとするとき，図7．から明らかに，Aは ①③④ の③を通ってBに，Bは直接Aに，それぞれ到達可能であるから，それらの間の連結は図8のようになる。（注意：結節点は，test tree に於て，ⓐ矢印が合流している状態，ⓑその状態を含む box の種類（どんな状態が含まれているか），の2つの要素で特長づけられるもので，そのどちらが違っても同じ結節点とは見なされない。）この図のように，loop が存在する場合は，"結節点の無限の連なり"が存在するわけであるから，明らかにτ-有界ではない。（g_3，g_4 のどちらも

最終状態でない場合は τ-有界となるが，その場合は q_3，q_4 は ϕ-状態となり，1. で述べたように，出力図 G には含まれない。

命題 3. test tree に結節点がある場合，P が τ-有界であるための必要充分条件は，結節点間の連結を示すグラフに loop が存在しないことである。

証明。τ-有界でないためには，結節点の無限の連なりが必要であることは test tree の構成から明らかであるが，結節点の種類は有限（実際，G の状態数を n とすると高々 $\sum_{i=1}^{n} {}_{n}C_{i}$）だから，結節点間の連結を示すグラフに loop が必要である。

4.（ϵ-free でない場合）　出力図 G に，無出力 ϵ をともなう遷移がある場合は，そのような遷移を，test tree の各 box の中に書けばよい。図 10. は図 9. の G_3 の test tree である。$\boxed{① \longrightarrow ②}$ は ① から ② へ無出力の遷移があることを示す。$\boxed{① \to ②}$ の ② は結節点である。これを A，$\boxed{◎}$ を B とすれば，結節点間の連結は図 11. のようになる。τ-有界性の判定規準は，命題 1, 3, と同様であり，図 11. は loop をなすから，P は τ-有界ではない。

以上により次の定理が成り立つ。

定理 2. 任意の gsm M と正規集合のペア（M, L）について，M が L に対して有限義解読可能か否かは決定可能である。

§4. 次数の決定.

次に，正規集合 L が M-有界である場合，解読可能性の次数がいくらであるかを決定することが可能であることを示す。

これは，test tree を変形することによっても求めることができるが，ここでは他の問題（例えば cellular automata）との関連で，L が正規集合であるとき，$D_2^M(L)$，$D_3^M(L)$，…… が全て正規集合となることを示すことによって，次数の判定が可解であることを証明する。

補題 1.　任意の正規集合 P と，短縮 homomorphism τ について，P の中での極大 τ-1 義正規集合 $\hat{P}$，すなわち

① $\hat{P} \subset P$　② $\hat{P}$ は τ-1 義　③ $\tau(\hat{P}) = \tau(P)$　④ $\hat{P}$：正規集合

をすべて満足する $\hat{P}$ が少くとも 1 つ存在し，かつ実際に構成可能である。

証明。　実際の構成法をのべる。

1．正規集合 P を受理する有限オートマトン B と，短縮 homomorphism τ とから，test tree をつくる。test tree にあらわれる box の種類を $b_0(=\{g_0\})$，b_1，b_2，… $\in 2^{K_B}$ とする。各 box の中のそれぞれの状態を (b_i, g_j) であらわす。(b_i, g_j) は box b_i の中の状態 g_j という意味である。$(g_j \in b_i)$　b_i を (b_i, g_j) の b-成分，g_j を (b_i, g_j) の g-成分と呼ぶことにする。

test tree の各矢印に対応する入力文字を書き込み，各 (b_i, g_j) を 1 つの独立した状態と見なせば，これは，もとの B と等価なオートマトンである。（但し，g-成分が B の最終状態であるような (b_i, g_j) を最終状態とする。）実際，g-成分が等しい状態は全て等価である。このようなオートマトンを redundant automaton と呼ぶ。

図 13. は図 12. で与えられた B と τ から作られた redundant automaton である。box は $b_0=\{g_0\}$，$b_1=\{g_1, g_3\}$，$b_2=\{g_2, g_3, g_4\}$，$b_3=\{g_0, g_3, g_4\}$ $b_4=\{g_1, g_3, g_4\}$，$b_5=\{g_3, g_4\}$ の 6 種類である。

2．次に，redundant automaton に於ける結節点への遷移のうち，任意の 1 つの遷移（矢印）だけを残して，他は消す。同時に，test tree の各 box に 2 つ以上の最終状態が含まれている時は，各 box について任意にその中の 1 つを指定して，これを新しいオートマトンの最終状態とする。このようにしてできたオートマトンは，その test tree に結節点をもたず，かつその各 box には高々 1 つの最終状態が含まれているにすぎない。

図13. では (b_2, q_4) 及び (b_4, q_3) が終節点であるから，$(b_1, q_1) \xrightarrow{t_2} (b_2, q_4)$, $(b_3, q_0) \xrightarrow{t_1} (b_4, q_3)$，$(b_4, q_1) \xrightarrow{t_2} (b_2, q_4)$ の各遷移を消し，又同時に，最終状態(◎で示す)として，(b_1, q_1), (b_2, q_2), (b_3, q_3), (b_4, q_3), (b_5, q_3) を指定したのが図14.である。図15.は図14.における同じboxの繰り返しをなくし，同じ状態を1つにまとめたものである。したがって，図15.のオートマトンのtest treeが図14.である。

③、このようにしてできた新しいオートマトンを $\hat{B}$ とする。オートマトン $\hat{B}$ は B のredundant automatonからいくつかの遷移を消してできたもので，しかもその最終状態の集合は，redundant automatonの最終状態の集合の部分集合である。したがって，$\hat{B}$ で受理される正規集合を $\hat{P}$ とすれば，明らかに $\hat{P} \subset P$ となる。又，$\hat{B}$ と τ からつくられるtest treeは，$\hat{B}$ の構成から明らかなように，各boxに高々1つの最終状態しか含まない。したがって，$\hat{P}$ は τ-1義である。更に，B のtest treeで最終状態を含んでいるようなboxに対応する $\hat{B}$ のtest treeの各boxは必ず最終状態を含んでいる。したがって，$\tau(P) \subset \tau(\hat{P})$ は明らかである。又，$\hat{P} \subset P$ より $\tau(\hat{P}) \subset \tau(P)$。故に $\tau(P) = \tau(\hat{P})$

よって，①②③④を満たす $\hat{P}$ の存在が，構成的に証明された。Q.E.D.

補題2. $D^{\tau}_{n+1}(P) = D^{\tau}_n(P) \cap \tau^{-1}\tau \cdot D^{\tau}_n(D^{\tau}_n(P) - \widehat{D^{\tau}_n(P)})$

$(P \subset T^*, \quad n = 1, 2, 3, \cdots)$

但し，$\widehat{D^{\tau}_n(P)}$ は，$D^{\tau}_n(P)$ の中での任意の極大 τ-1義集合

又 $\tau^{-1}(A) = \{ x \in T^* \mid \tau(x) \in A \}$

証明。 $x \in D^{\tau}_{n+1}(P)$ とする。

$D^{\tau}_{n+1}(P) \subset D^{\tau}_n(P)$ だから，$\tau(x) \in \tau \cdot D^{\tau}_n(D^{\tau}_n(P) - \widehat{D^{\tau}_n(P)})$ を証明すればよい。

仮定より，$\exists x_1, x_2, \cdots, x_n \in D^{\tau}_n(P)$ $(x_i \neq x,\ x_i \neq x_j \text{ if } i \neq j,\ i, j = 1, 2, \cdots, n)$

$\tau(x_i) = \tau(x) \quad \forall i = 1, \cdots, n$

である。

① $x \in \widehat{D^{\tau}_n(P)}$ のとき.

$\widehat{D^{\tau}_n(P)}$ の意味より，$\forall x' \in \widehat{D^{\tau}_n(P)}$, $\tau(x') \neq \tau(x)$

故に，$x_i \in D^{\tau}_n(P) - \widehat{D^{\tau}_n(P)} \quad \forall i = 1, \cdots, n$

よって，$x_i \in D^{\tau}_n(D^{\tau}_n(P) - \widehat{D^{\tau}_n(P)}) \quad \forall i = 1, \cdots, n$

故に，$\tau(x) = \tau(x_i) \in \tau \cdot D^{\tau}_n(D^{\tau}_n(P) - \widehat{D^{\tau}_n(P)})$

② $x \in D_n^\tau(P) - \widehat{D_n^\tau(P)}$ のとき。

$\widehat{D_n^\tau(P)}$ には，$\tau(x') = \tau(x)$ なる x' は1つしか含まれないから，

$x' = x_n$ とすると，　$x_1, x_2, \cdots, x_{n-1} \in D_n^\tau(P) - \widehat{D_n^\tau(P)}$

故に，$x \in D_n^\tau(D_n^\tau(P) - \widehat{D_n^\tau(P)})$

よって，$\tau(x) \in \tau \cdot D_n^\tau(D_n^\tau(P) - \widehat{D_n^\tau(P)})$

逆に，$x \in D_n^\tau(P) \cap \tau^{-1}\tau \cdot D_n^\tau(D_n^\tau(P) - \widehat{D_n^\tau(P)})$

すなわち，　$x \in D_n^\tau(P)$ ……①

かつ，$\tau(x) \in \tau \cdot D_n^\tau(D_n^\tau(P) - \widehat{D_n^\tau(P)})$ ……②

とする。

②より，$\exists x_1 \in D_n^\tau(D_n^\tau(P) - \widehat{D_n^\tau(P)})$ ……③

$\tau(x) = \tau(x_1)$ ……④

③より，$\exists x_2, x_3, \cdots x_n \in D_n^\tau(P) - \widehat{D_n^\tau(P)}$　($x_1 \neq x_j$, $x_i \neq x_j$ if $i \neq j$ 但し $i, j = 2, 3, \cdots, n$)

$\tau(x_1) = \tau(x_2) = \cdots\cdots = \tau(x_n)$ ……⑤

x が $x_1, x_2, \cdots, x_n$ のどれとも等しくないときは，① 及び $D_{n+1}^\tau(P)$ の定義により，

$x \in D_{n+1}^\tau(P)$。

$\exists x_i$, $x = x_i$ のとき，① 及び $\widehat{D_n^\tau(P)}$ の意味より

$\exists x_{n+1} \in \widehat{D_n^\tau(P)}$,　$\tau(x) = \tau(x_{n+1})$ ……⑥

$x_1, x_2, \cdots, x_i(=x), \cdots, x_n \in D_n^\tau(P) - \widehat{D_n^\tau(P)}$

$x_{n+1} \in \widehat{D_n^\tau(P)}$

だから，⑤⑥より，$x \in D_{n+1}^\tau(P)$　　Q.E.D.

（注意；右辺第1項の $D_n^\tau(P)$ は P でおきかえてもよい）

補題3．P が正規集合であるとき，$D_1^\tau(P)(=P)$，$D_2^\tau(P)$，$D_3^\tau(P)$ …… は全て正規集合であり，かつ構成可能である。

証明。　数学的帰納法による。

定義により，$D_1^\tau(P) = P$ だから，任意の正規集合 P について $D_1^\tau(P)$ は正規集合である。今，任意の正規集合 P について，$D_n^\tau(P)$ が正規集合であるとすると，補題1．により，$D_n^\tau(P)$ の中での極大 τ-1義正規集合 $\widehat{D_n^\tau(P)}$ が存在する。したがって，$D_n^\tau(P) - \widehat{D_n^\tau(P)}$ は正規集合である。よって，再びもとの仮定から $D_n^\tau(D_n^\tau(P) - \widehat{D_n^\tau(P)})$ は正規集合となり，正規集合のクラスは，homomorphism τ 及びその逆写像 τ^{-1} について閉じているから，$\tau^{-1}\tau \cdot D_n^\tau(D_n^\tau(P) - \widehat{D_n^\tau(P)})$ は正規集合となる。

よって，補題2.により，$D^{\tau}_{n+1}(\mathbb{P}) = D^{\tau}_{n}(\mathbb{P}) \cap \tau^{-1}\tau \cdot D^{\tau}_{n}(D^{\tau}_{n}(\mathbb{P}) - \widehat{D^{\tau}_{n}(\mathbb{P})})$ は正規集合である。

又，$D^{\tau}_{n}(\mathbb{P})$が任意の正規集合$\mathbb{P}$について構成可能ならば，補題1.により$\widehat{D^{\tau}_{n}(\mathbb{P})}$ は $D^{\tau}_{n}(\mathbb{P})$ 及び τ より構成可能だから，$D^{\tau}_{n+1}(\mathbb{P})$は構成可能である。 Q.E.D.

定理3. 任意のgsm $\mathbb{M}$と正規集合Lの組 $(\mathbb{M}, L)$ について，

$D^{\mathbb{M}}_{1}(L)(=L)$，$D^{\mathbb{M}}_{2}(L)$，$D^{\mathbb{M}}_{3}(L)$ …… は全て正規集合であり，かつ $\mathbb{M}$ とLより構成可能である。

証明。 $\mathbb{P}$とLとはhomomorphism σにより1対1に対応している。

σ^{-1}をσの逆写像(一般にhomomorphism)とすると，$\mathbb{M}(x) = \tau\sigma^{-1}(x)$ $\forall x \in L$

よって，$D^{\mathbb{M}}_{n}(L) = D^{\tau\sigma^{-1}}_{n}(L) = \sigma \cdot D^{\tau}_{n}(\sigma^{-1}L) = \sigma D^{\tau}_{n}(\mathbb{P})$ となる。

故に，補題3.により$D^{\mathbb{M}}_{n}(L)$は正規集合で，かつ構成可能。

$$\begin{tikzcd} L \arrow[r, shift left, "\sigma^{-1}"] \arrow[dr, "\mathbb{M}"'] & \mathbb{P} \arrow[l, shift left, "\sigma"] \arrow[d, "\tau"] \\ & \mathbb{M}(L) \end{tikzcd}$$

系1. 任意の正整数nについて，$\mathbb{M}$が正規集合Lに対してn義解読可能か否か決定可能である。

系2. $\mathbb{M}$が正規集合Lに対して情報無損失か否か決定可能である。

系3. 任意の正整数nについて，正規集合Lが極大$\mathbb{M}$-n義集合か，極大$\mathbb{M}$-無損失集合か，判定可能である。

系4. Lを任意の文脈自由言語，MをL⊂Mなる任意の正規集合とするとき，任意の正整数nについて，LがMをヒントとして$\mathbb{M}$-n義であるか否かは決定可能である。

証明。 系1.は定義により $D^{\mathbb{M}}_{n}(L) \neq \phi$，$D^{\mathbb{M}}_{n+1}(L) = \phi$ か否か調べればよい。$D^{\mathbb{M}}_{n}(L)$，$D^{\mathbb{M}}_{n+1}(L)$は構成可能な正規集合だから，これは決定可能である。

系2.は定義により，すべての$Q_j \in K_{\mathbb{M}}$について，$L \cap R(Q_j)$が$\mathbb{M}$-1義か否かを調べればよい。系3.についても同様。

系4. は定義により，$D^{M}_{n+1}(M)\cap L=\phi$，$D^{M}_{n}(M)\cap L\neq\phi$ か否かを調べればよい。正規集合と文脈自由言語との共通部分は文脈自由言語であり，ϕか否かは決定可能である。 Q.E.D.

定理4. 任意のgsm Mと正規集合Lの組（M, L）について，MのLに対する有限義解読可能性の次数を求めるアルゴリズムが存在する。

証明。定理2. 及び定理3. の系1. より明らか。

Lを文脈自由言語，Mを$L\subset M$なる正規集合とするとき，Lが正規集合MをヒントとしてM-有界か否か，すなわち $L\cap D^{M}_{n+1}(M)=\phi$ なる $n\geq 1$ が存在するか否か，が決定可能かどうかは定理3. からではわからない。しかし，test treeを応用することにより，これを判定するアルゴリズムが存在することを示すことができる。

以下，そのアルゴリズムをのべる。

（以下省略）

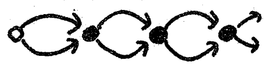
文献

[1] 佐藤興二：順序回路の正規集合に関する情報無損失性 通信学会研究会資料（1969.4 A69−8）
[2] Ал.А.Марков; ДАН, СССР 1960～1962 に出たいくつかの論文
[3] Ю.В. Глебский; ДАН. СССР 141, 5, 1961
[4] В.И, Левенштейн; ДАН. СССР 142, 6, 1962
[5] S.Ginsburg; The Mathematical Theory of context free Language McGraw-Hill

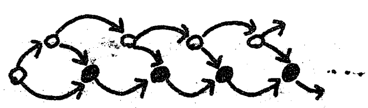
註1) K_M：内部状態の集合，Σ：入力アルファベット，Δ：出力アルファベット
δ_M：状態遷移函数 $K_M\times\Sigma\to K$，λ_M：出力函数 $K_M\times\Sigma\to\Delta^*$
Q_0：初期状態 $\in K_M$，δ_M,λ_Mを$K_M\times\Sigma^*$上に自然に拡張したものも，δ_M，λ_Mであらわす。$\lambda_M(Q_0,x)$をxの函数($x\in\Sigma^*$)と見なしたとき，$M(x)$であらわす。$M(L)=\{y\in\Delta^* \mid \exists x\in L, M(x)=y\}$である。

註2) $K_A,\Sigma,\delta_A,q_0\in K_A$は$M$の場合と同様。$F\subset K_A$は最終状態の集合

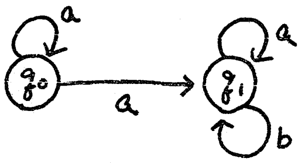
註3) "結節点の無限の連なり"は大ざっぱに言って，2種類に分けられる。右はその模式図である。図a.の場合，出力系列の長さが増すにつれて対応する入力系列の数は指数函数的に増すが，図bの場合は，linearに増していくに過ぎない。Gが強連結の場合は，常に図a.のようになり，図bは強連結でない場合に限られる。下はその例である。



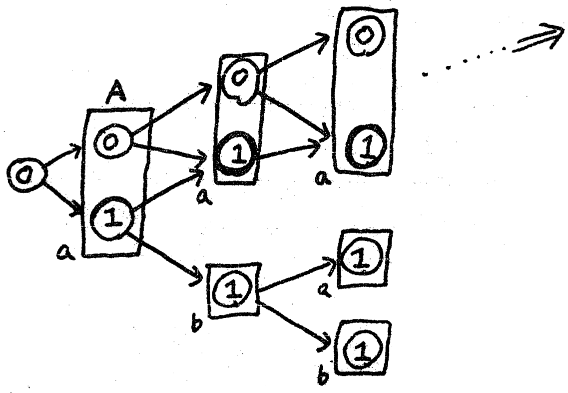
図a.

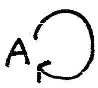


図b.



(G)





(test tree of G)

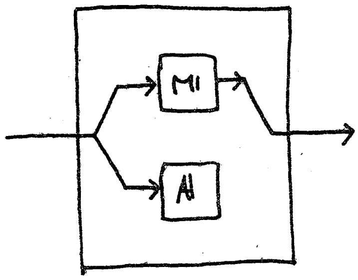


図1. M1×A1

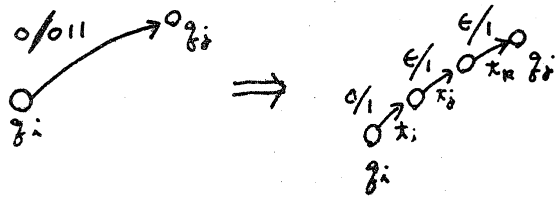


図 2.

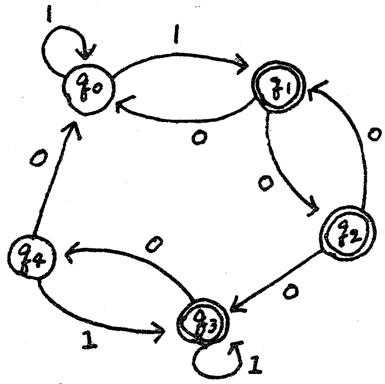


図 3. G_1

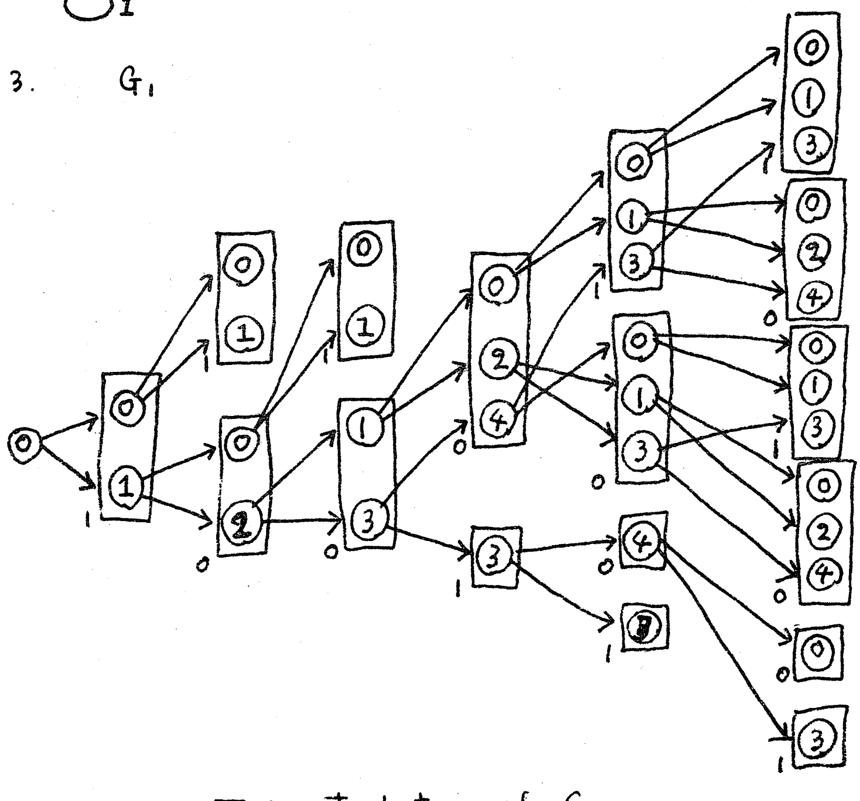


図 4. Test tree of G_1

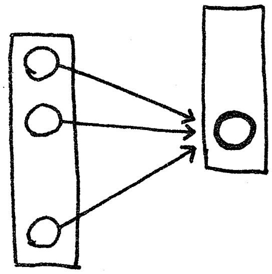


図5. 結節点

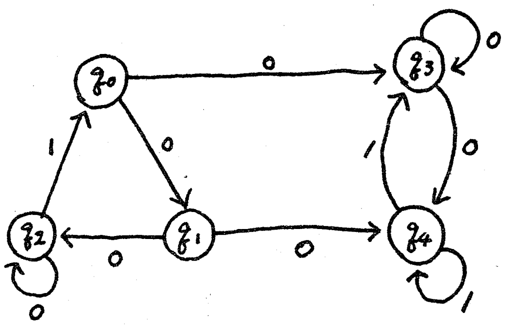


図6. G_2

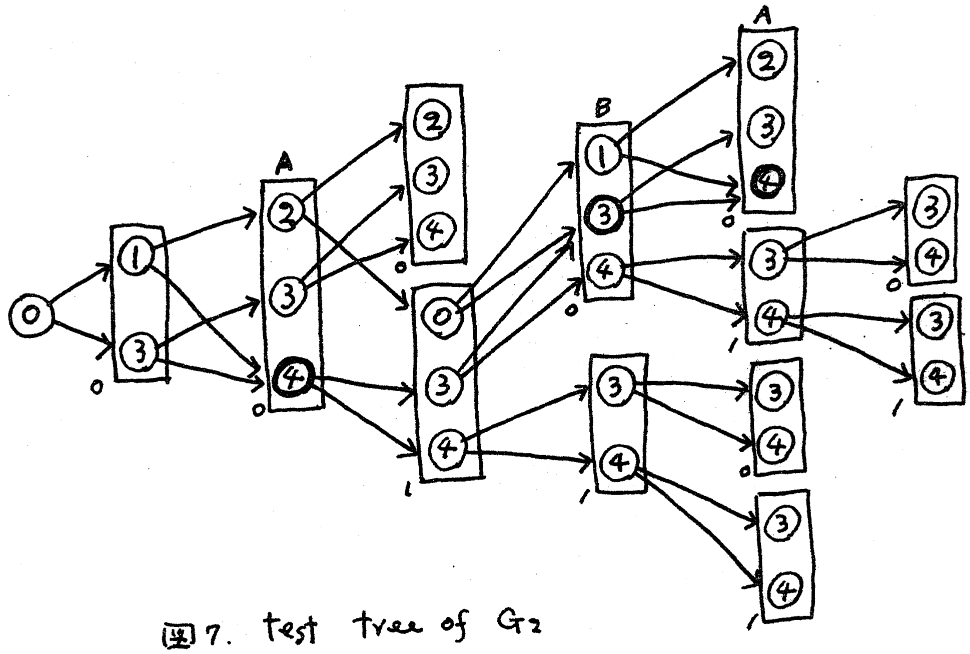


図7. test tree of G_2

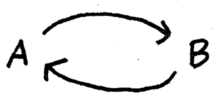


図8. 結節点間の連結
を示すグラフ

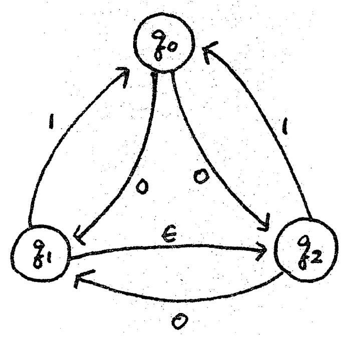


図 9. G_3

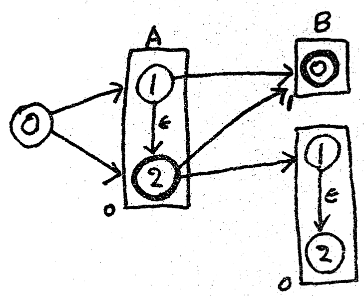


図 10. test tree of G_3

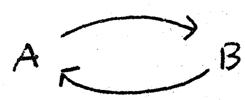


図 11.

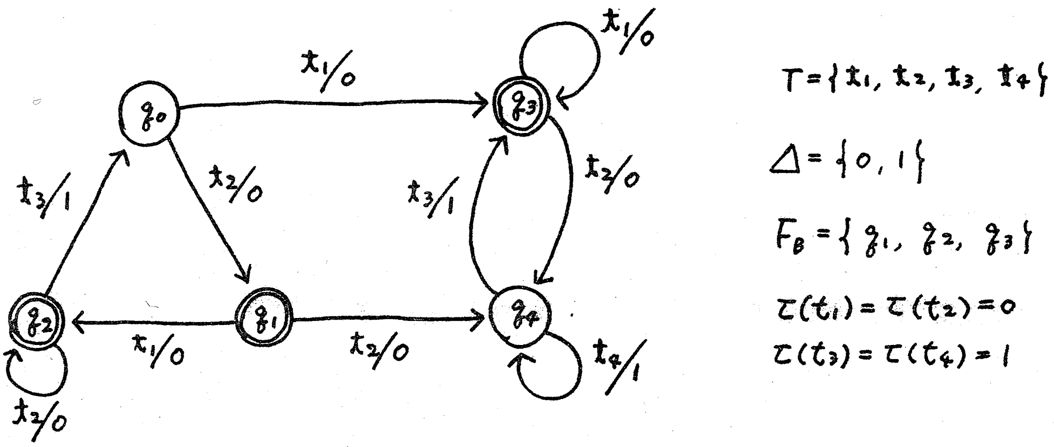


図12. PCT*を定義するオートマトンBおよびτによる出力
φ-状態は省略されている。

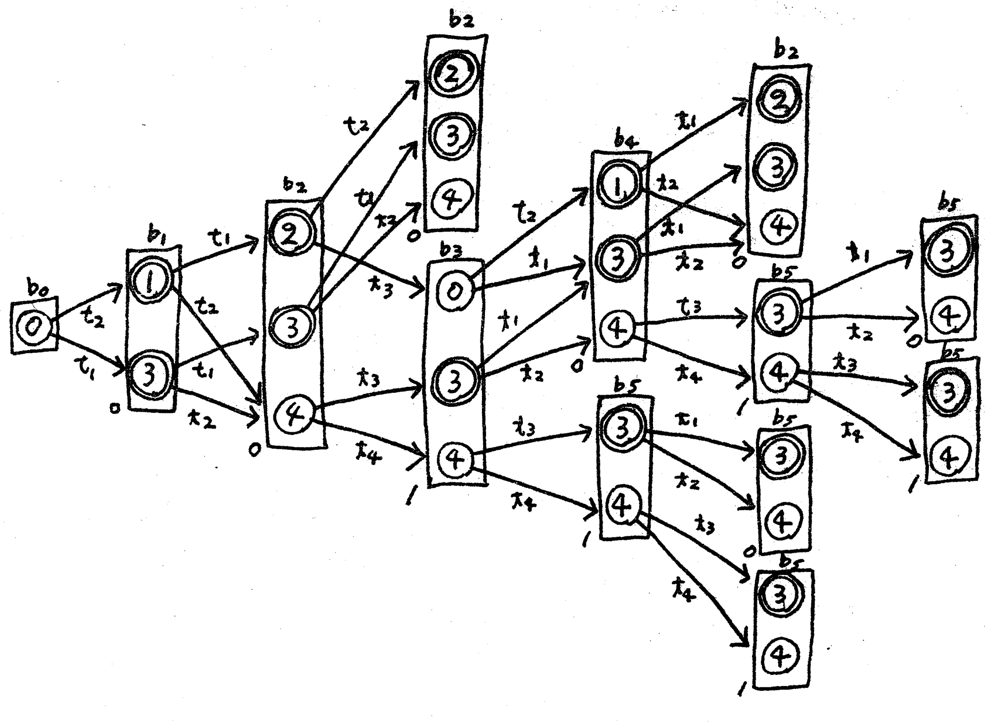


図13.

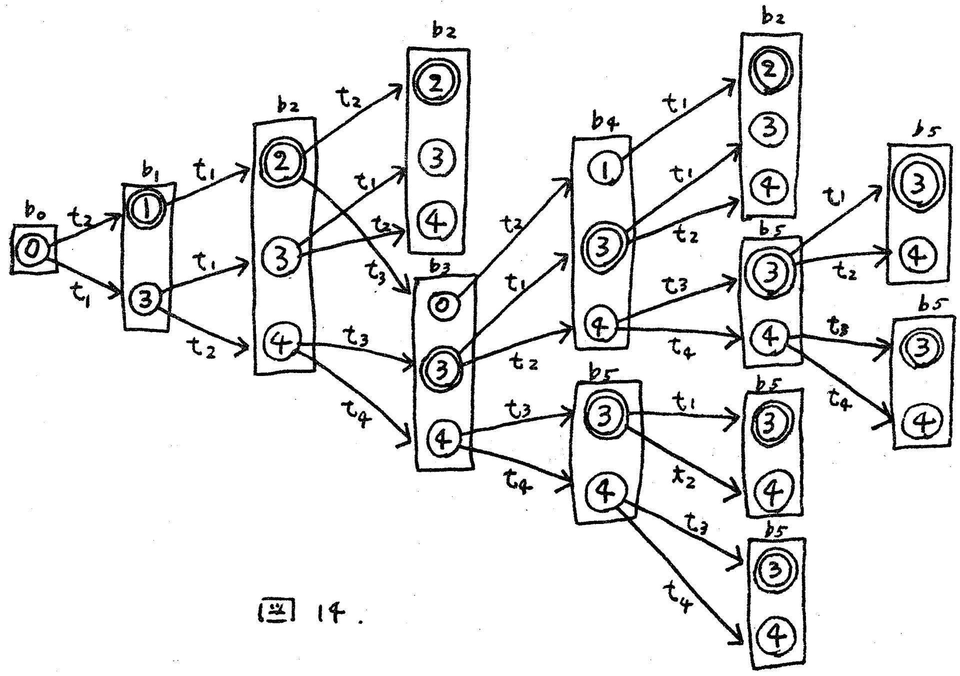


図14.

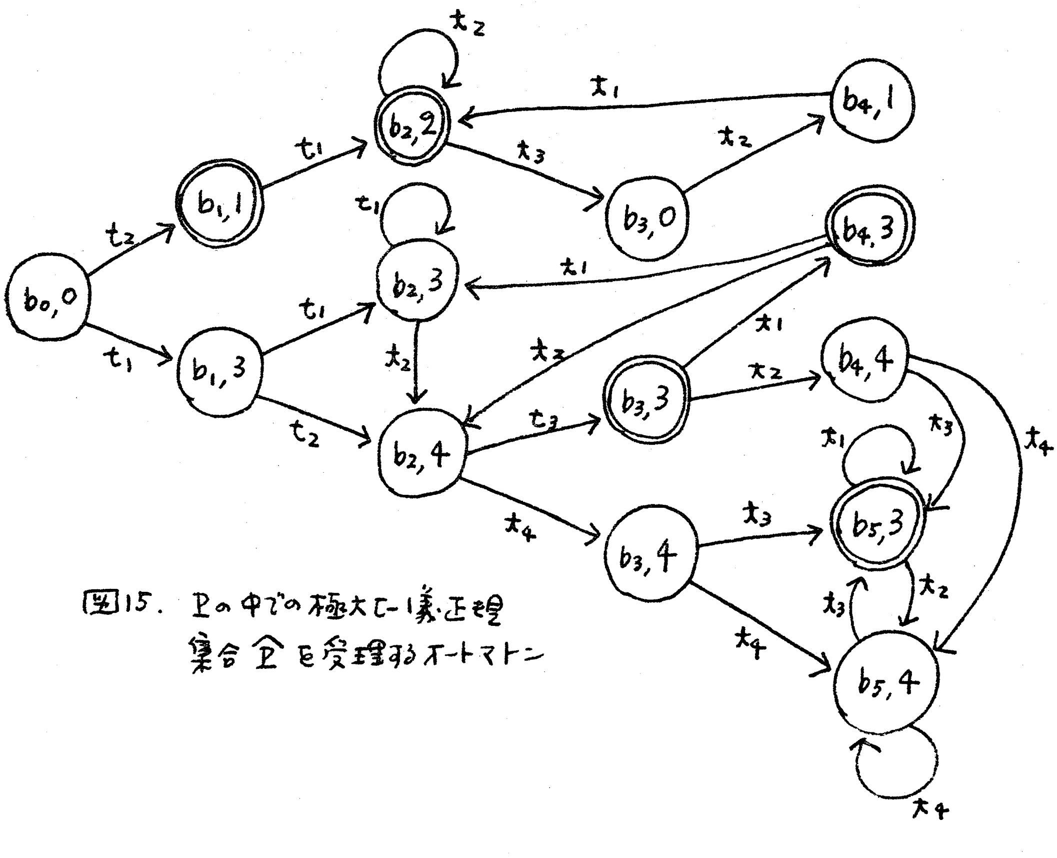


図15. Pの中での極大で一様正規集合 $\hat{P}$ を受理するオートマトン